Link to article: https://discover.claromentis.com/knowledgebase/articles/572

Integrating with existing Identity Providers (SSO) and User Directories

Introduction

The Claromentis framework fully supports integration with existing user directories and identify providers. In short, integration with user directories allows for the easy provisioning and management of user profiles in Claromentis. In addition to this, there are a variety of different ways to integrate with an existing Identity Provider (IDP) to setup Single Sign-On (SSO) for users, so that their method of logon is as seamless as possible.

This article covers some of the benefits of integrating with an existing IDP and setting up SSO, as well as outlining how this is achieved. If you have any further questions, please reach out to your Account Manager or Project Manager and we'll be happy to advise further via email or a scheduled technical call.

User Directory Integration - Benefits

Here are just some of the many benefits of integrating with an existing User Directory:

- Allows for centralised user management from an existing user directory
- Existing user profiles, and the information contained within each profile, can be automatically synchronised from the User Directory to Claromentis.
- Claromentis can pre-populate user information and profiles, ready for your system to be launched! This information is then synchronised at regular intervals (for example hourly, daily or weekly) so that any information amended in the User Directory is automatically updated to Claromentis.
- Facilitate the use of local Claromentis accounts and external user directory accounts Claromentis local accounts can still be used once the integration in place. This allows for internal users and external users to both gain access to the same system and content.
- Control Access with Security Groups / OU's The Administrator has the power to only allow certain security groups or organisational units to have access to the Digital Workplace. The Administrator therefore has full control over who can/cannot login to the system.
- Group management and access control from existing user directory structure Claromentis can be configured to use an existing user directory structure to create permission groups or roles, which help limit access to content and applications within Claromentis. This allows permission management to be controlled directly from the user directory and usually fits in with existing methods for granting and denying access.
- Users can sign-in using existing network/computer or IDP credentials Corporate users will already have a set of network credentials that are used to access existing resources. By integrating with a user directory, these exact same credentials can be used to access the Intranet.

Identity Provider (SSO) Integration - Benefits

Here are just some of the many benefits of integrating with an existing SSO or Identity Provider:

- Configuring SSO will allow users who are logged in to a network computer to simply open a web browser and be immediately logged in to the Intranet under their current username and password. Single Sign-On allows your users to access the Claromentis intranet system without needing to enter a username or password.
- The credentials are obtained automatically, based upon the user currently logged in to the computer being used to access the site. For users, this gives them a seamless experience and gets them to the content quickly and efficiently. For administrators, it reduces the amount of support requests relating to access credentials. If access is permitted to the site from outside the organisational network, users will still be prompted to enter credentials as usual and will still be able to login using directory credentials.
- Once a user leaves an organisation, access can easily be revoked in the Identity Provider and the user will no longer be able to login to the Claromentis system.

Integration Options

Integrating your existing User Directory and Identity Provider is possible when Claromentis is deployed On Premise as well as on our SaaS/Cloud environments.

Here are a few examples of our two most common integrations, however we will advise on the recommended setup for each client, depending on your requirements and during the initial stages of the project. If you have any questions, please contact your account manager who will be happy to pass your queries onto our technical team.

On Premise - LDAP(S) & NTLM/Kerberos

User Directory Synchronisation: When hosting Claromentis inside your existing infrastructure, it's possible for Claromentis to make a direct connection to your user directory's controller server using LDAP or LDAPS protocols. This connection is then used to obtain and populate the required information inside Claromentis' user profiles. This is the quickest and simplest integration method to implement, and requires no additional setup beyond the initial configuration details.

SSO (Single Sign-On): As the on premise environment is likely a member of the organisations domain, it's therefore very simple for the Claromentis team to setup NTLM/Kerberos authentication by utilising the authentication methods built into IIS web server. Therefore a Windows web server is recommend if Claromentis is a) On Premise and b) Requires SSO using NTLM/Kerberos.

Note: If hosting on Linux is a requirement for the on premise environment, a setup similar to the SaaS/Cloud Hosted example below is advised.

SaaS/Cloud - LDAP(S) & SAML

User Directory Synchronisation: We recommend that a direct connection is setup between the Claromentis SaaS/Cloud hosted server and the client's User Directory.

This is a secure implementation as we insist on the following conditions being met:

- The user account provisioned for the synchronisation between Claromentis and the domain controller should only provide read-only access.
- Only secure LDAPS protocol/ports should be used (TCP 636/TCP 3269) and the SSL certificate on the DC must be valid
- Incoming ACL/Firewall rules will need to be implemented for the TCP port(s) listed above and these should be IP restricted to an IP address which is exclusive to the client's Saas/Cloud hosted environment (we'll provide further details, including the Static IP address(es) during the initial project launch).

SSO (Single Sign-On): As the SaaS/Cloud hosted environment is not a member of the client's domain, it's not possible to use Windows Authentication for SSO. Instead we recommend that SSO is instead implemented by using a directory independent identity provider that supports SAML (for example ADFS).

Supported User Directory & Identity Providers

User Directories

• Microsoft Active Directory (2003, 2008, 2012, 2016)

• NetIQ eDirectory (previously known as Novell eDirectory)

• OpenLDAP

Identity Providers

• Windows Authentication (NTLM/Kerberos)

• Any IDP that supports SAML 2.0 (ADFS, Okta, Duo, Centrify, One Login etc.)

• Any IDP that supports OAuth (Google, Microsoft, Twitter, Facebook etc.)

Custom User Directories / Identity Providers

The attribute fields that Claromentis uses to query the directory server are largely customisable, and therefore it is technically possible for Claromentis to integrate with a non-standard user directory or identity provider and we have a custom development team who can assist with this process.

If you are using a directory system that is not mentioned in the requirements section above, please contact your account manager or project manager to arrange a technical call to go through your requirements and to see what's possible!

Last modified on 15 November 2019 by Michael Christian

Created on 14 May 2019 by Will Emmerson
Tags: active, directory, google, ldap, saml, SSO, idp, ldaps, novell, e-directory, oauth, gsuite